Aufgaben des Sicherheitsmoduls

Das Sicherheitsmodul hat folgende Aufgaben:

- Sicherung der Authentizität von Transaktionsdaten, d.h. eine Verifikation der Transaktionsdaten zeigt, ob diese durch das Sicherheitsmodul mit der referenzierten Seriennummer erstellt wurden.
- Sicherung der Vollständigkeit der Transaktionsdaten, d.h. die Transaktionsnummern sind lückenlos aufsteigend und fehlende Transaktionen können erkannt werden.

Ein Sicherheitsmodul muss zur Erfüllung dieser Aufgaben hinreichend resistent gegen eine Reihe von Angriffen sein. Zur Identifikation von relevanten Angriffen, die vom Sicherheitsmodul abgewehrt werden sollen, werden im Rahmen einer Bedrohungsanalyse zunächst systematisch Sicherheitsziele entwickelt, die von einem Sicherheitsmodul oder in der Einsatzumgebung umgesetzt werden müssen. Aus den Sicherheitszielen des Sicherheitsmoduls werden anschließend formale Anforderungen an die Sicherheitsfunktionen des Sicherheitsmoduls abgeleitet, welche durch eine vom BSI anerkannte Prüfstelle entsprechend einer International standardisierten Vorgehensweise evaluiert und durch das BSI zertifiziert werden können.

Die folgende Bedrohungsanalyse ist ein Auszug aus dem BSI-Schutzprofil „Cash Register Security Module Application“, welches auf dem BSI-Schutzprofil „Cryptographic Service Provider“ aufbaut.

Transaktionen

Zur Sicherung der Transaktionen erzeugt das Sicherheitsmodul aus Transaktionsdaten eine Sequenz von Transaktionsdatensätzen.

Transaktionsdaten: Die unsignierten Daten, die von der Kasse an das Sicherheitsmodul übertragen werden.

Transaktionsdatensätze: Die vom Sicherheitsmodul erzeugten Datensätze aus signierten Transaktionsdaten.

Eine **Sequenz von Transaktionsdatensätzen** ist eine Folge von Transaktionsdatensätzen mit fortlaufender Transaktionsnummer und aufsteigendem Zeitpunkt des Vorgangsbeginns.

Bedrohungen

Die folgenden Bedrohungen müssen durch Sicherheitsziele des Sicherheitsmoduls oder der Einsatzumgebung adressiert werden.

T.EvadTDS Transaktionsdatensätze auslassen

Der Angreifer umgeht das Erzeugen von Transaktionsdatensätzen, indem er das Senden von Transaktionsdaten an das Sicherheitsmodul umgeht.

T.ManipTD Manipulation von Transaktionsdaten

Der Angreifer manipuliert die Transaktionsdaten, die von der Kasse an das Sicherheitsmodul gesendet werden oder erzeugt gefälschte Transaktionsdaten und sendet diese an das Sicherheitsmodul um falsche Transaktionsdatensätze zu erzeugen.

T.ManipTDTBS Manipulation von Transaktionsdaten vor Signaturerstellung

Der Angreifer erzeugt gefälschte Transaktionsdaten oder manipuliert Transaktionsdaten im Sicherheitsmodul, bevor diese signiert werden.

T.ManipTDS Manipulation von Transaktionsdatensätzen

Der Angreifer manipuliert exportierte Transaktionsdatensätze.

T.ManipTDSS Manipulation einer Sequenz von Transaktionsdatensätzen

Der Angreifer manipuliert eine exportierte Sequenz von Transaktionsdatensätzen.

T.ManipTime Manipulation der Zeitquelle

Der Angreifer manipuliert berechtigt oder unberechtigt die interne Zeit des Sicherheitsmoduls zur Erstellung von Zeitstempeln ohne, dass dieses erkannt wird.

T.ManipTN Manipulation der Transaktionsnummer

Der Angreifer manipuliert die internen Transaktionsnummern.

T.FaUpD Fehlerhafte Updates

Über ein unberechtigt erzeugtes, fehlerhaftes Update werden Angriffe auf das Sicherheitsmodul ermöglicht.

Organisatorische Sicherheitsrichtlinien

Hierbei handelt es sich um Grundvoraussetzungen für den sicheren Betrieb. Diese Voraussetzungen können durch Sicherheitsziele des Sicherheitsmoduls oder der Einsatzumgebung realisert werden.

OSP.SecCCRS Sichere Nutzung der Kasse

Der Steuerpflichtige soll ein Kassensystem nutzen, das digitale Grundaufzeichnungen und Belege erzeugt. Das Kassensystem soll alle rechtlich vorgeschriebenen Vorgänge einzeln, korrekt und vollständig sowie in Echtzeit aufzeichnen (s. AO §146a (1) Satz 1). Der Beleg soll den Zeitpunkt des Vorgangsbeginns sowie Abbruch bzw. Ende und die Transaktionsnummer enthalten, wie im Transaktionsdatensatz des Sicherheitsmoduls angegeben (s. KassenSichV §6 Satz 1).

OSP.CertSecDev Zertifizierte Sicherheitseinrichtung

Die Kasse und die Grundaufzeichnungen sollen von einer zertifizierten Sicherheitseinrichtung geschützt werden (s. AO §146a (1) Satz 2). Die Komponenten der zertifizierten

Sicherheitseinrichtung sollen nach den entsprechenden Technischen Richtlinien und Schutzprofilen des BSI zertifiziert werden.(s. AO §146a (3)).

OSP.SecMod Funktionalität des Sicherheitsmoduls

Das Sicherheitsmodul erzeugt jeweils einen Zeitstempel bei Beginn und Ende eines Vorgangs und vergibt eine Transaktionsnummer.

OSP.ProtDev Schutz der Kasse und technischen Sicherheitseinrichtung

Der Steuerpflichtige nutzt die Kasse vorschriftsmäßig (s. AO § 379 (1) Satz 1 Nr. 4) und schützt die Kasse und die technische Sicherheitseinrichtung (s. AO § 379 (1) Satz 1 Nr. 5).

OSP.ValidTDSS Gültigkeit einer Sequenz von Transaktionsdatensätzen

Eine Sequenz ist gültig, wenn (1) die Transaktionsdatensätze den Anforderungen in KassenSichV §2 genügen, (2) der Prüfwert eine gültige digitale Signatur darstellt, die vom Sicherheitsmodul erzeugt wurde, (3) die Transaktionsnummern der Sequenz lückenlos fortlaufend sind und (4) die Zeitpunkte des Vorgangsbeginns mit fortlaufenden Transaktionsnummern ansteigend sind.

OSP.Update Einspielen von Updates

Updates werden an das Sicherheitsmodul in verschlüsselter und durch den Herausgeber signierter Form geliefert. Das Sicherheitsmodul verifiziert die Authentizität des Updates vor der Speicherung des Updates. Das Sicherheitsmodul beschränkt das Einspielen von Updates auf den Administrator.

Annahmen

Annahmen über den Einsatz des Sicherheitsmoduls können in der Regel nicht ausschließlich technisch erzwungen werden.

A.CSP Kryptoprovider

Die Einsatzumgebung stellt einen zertifizierten Kryptoprovider zur Verfügung.

Hinweis: Der Kryptoprovider kann eine Komponente sein, die NICHT im Kassensystem eingebaut ist (Cloud).

A.ProtComm Schutz der Kommunikation

Die Einsatzumgebung schützt die Vertraulichkeit und Integrität der Kommunikation zwischen Sicherheitsmodul, Kassensystem und Kryptoprovider.

A.VerifTDS Prüfung einer Sequenz von Transaktionsdatensätzen

Die digitalen Signaturen, die Transaktionsnummern und die Zeitstempel werden verifiziert, um gefälschte oder fehlende Transaktionen zu entdecken. Das Zertifikat zur Verifikation der Signaturen wird auf sicherem Weg zum Prüfer übermittelt.

Sicherheitsziele für das Sicherheitsmodul

Die Sicherheitsziele müssen technisch mithilfe von Sicherheitsfunktionen durch das Sicherheitsmodul umgesetzt werden. Die Umsetzung der Sicherheitsziele sind Gegenstand der Zertifizierung.

O.TEE Test der externen Einheiten

Das Sicherheitsmodul soll testen, dass die Kasse und der Kryptoprovider an das Sicherheitsmodul angeschlossen sind. Die Erstellung von Transaktionsdatensätzen soll nur möglich sein, wenn die Tests erfolgreich sind. Für jeden fehlgeschlagenen Test werden Auditeinträge durch das Sicherheitsmodul erzeugt.

O.GenTDS Erzeugung von Transaktionsdatensätzen

Das Sicherheitsmodul erzeugt einen Transaktionsdatensatz aus den von der Kasse importierten Transaktionsdaten, dem Vorgangsbeginn und End- bzw. Abbruchzeitpunkten, der Transaktionsnummer und einer digitalen Signatur über die Transaktionsdaten. Das Sicherheitsmodul muss sicherstellen, dass die Transaktionsdatensätze mit lückenlos fortlaufenden Transaktionsnummern erzeugt werden, sowie dass die Zeitpunkte des Vorgangsbeginns mit fortlaufenden Transaktionsnummer ansteigend sind.

O.ExpTDS Export von Transaktionsdatensätzen

Jeder Transaktionsdatensatz wird vom Sicherheitsmodul an die Kasse zur Belegerzeugung und Archivierung exportiert.

O.IAA Identifikation, Authentisierung und Zugriffskontrolle

Das Sicherheitsmodul muss die externen Einheiten Kasse und Kryptoprovider identifizieren und testen. Der Administrator muss durch ein Passwort identifiziert werden.

O.SecMan Verwaltung von Sicherheitsparametern

Nur Administratoren dürfen Sicherheitsparameter einschließlich der Zeitquelle setzen. Die Erzeugung von Transaktionsnummern darf nicht durch eine Verwaltungsfunktion steuerbar sein.

O.Audit Audit

Das Sicherheitsmodul implementiert eine Funktion, um die Nutzung von Sicherheitsfunktionen durch Erkennen, Aufzeichnen und Speichern von relevanten Aktivitäten nachvollziehbar zu machen. Das schließt insbesondere die Verwaltung der Zeitquellen und der Auditeinträge ein.

O.TST Selbsttest und Fehlerzustand

Das Sicherheitsmodul muss Selbsttests durchführen. Das Sicherheitsmodul wird in einen Fehlerzustand überführt, wenn ein Selbsttest fehlschlägt, die Zeitquelle nicht verfügbar ist, oder ein Test des Kassensystems oder des Kryptoproviders fehlschlägt.

O.SecUpCP Sicheres Laden und Autorisierung von Updates

Das Sicherheitsmodul muss verschlüsselte Updates verifizieren und entschlüsselt ausschließlich authentische Updates, bevor dieses lokal gespeichert wird. Das Sicherheitsmodul darf ausschließlich dem Administrator das Einspielen des Updates erlauben.

Sicherheitsziele für die Umgebung

Diese Sicherheitsziele können nicht mithilfe von Sicherheitsfunktionen durch das Sicherheitsmodul umgesetzt werden, sondern müssen durch die Einsatzumgebung realisiert werden. Das Sicherheitsmodul wird nur dann im zertfizierten Modus betrieben, wenn die Sicherheitsziele der Umgebung erfüllt sind.

OE.CCRS Vertrauenswürdiges Kassensystem

Der Steuerpflichtige soll ein Kassensystem nutzen, das alle gesetzlich geforderten Transaktionsdaten einzeln, korrekt, vollständig und in Echtzeit zur Erzeugung von Transaktionsdatensätzen an das Sicherheitsmodul weiterleitet. Die Übermittlung von Vorgangsbeginn und -ende bzw. -abbruch muss zeitnah durch die Kasse erfolgen.

OE.CSP Kryptoprovider

Die Umgebung muss sicherstellen, dass der Kryptoprovider nach dem Schutzprofil Cryptographic Service Provider zertifiziert ist. Der Steuerpflichtige muss sicherstellen, dass der Kryptoprovider mit einem Signaturschlüssel und einem gültigen Zertifikat, das auf den Steuerpflichtigen verweist, ausgestattet ist. Das Zertifikat wird auf sicherem Weg dem Prüfer zur Verfügung gestellt.

Hinweis: Das Zertifikat muss nicht die Identität des Steuerpflichtigen enthalten, aber das Zertifikat muss eindeutig einem Steuerpflichtigen zuzuordnen sein.

OE.StorMed Speichermedium

Der Steuerpflichtige muss ein nach Technischen Richtlinien zertifiziertes Speichermedium einsetzen, um die Langzeitverfügbarkeit der archivierten Transaktionsdatensätze sicherzustellen.

OE.VerifTDSS Verifikation von Transaktionsdatensätzen

Die Einsatzumgebung soll die Gültigkeit von Transaktionsdatensätzen durch Prüfung der digitalen Signatur, der lückenlos fortlaufenden Transaktionsnummern, sowie der mit fortlaufenden Transaktionsnummern ansteigenden Zeitpunkte des Vorgangsbeginns prüfen.

OE.AvailAudit Verfügbarkeit von Auditdaten

Der Administrator muss die Verfügbarkeit der exportierten Auditdaten sicherstellen.

OE.SecEnv Sichere Einsatzumgebung

Die Kasse, das Speichermedium, der Kryptoprovider und das Sicherheitsmodul müssen in einer sicheren Einsatzumgebung betrieben werden, die gegen Manipulation, Störung und

Kompromittierung geschützt wird. Die Integrität der Kommunikation zwischen Kasse und Sicherheitsmodul bzw. Sicherheitsmodul und Kryptoprovider muss geschützt werden.

OE.SUCP Signierte Updates

Der Hersteller gibt verschlüsselte und digital signierte Updates heraus.

Sicherheitsbewertung

Alle Bedrohungen, organisatorische Sicherheitsmaßnahmen und Annahmen müssen durch Sicherheitsziele des Sicherheitsmoduls oder der Einsatzumgebung abgedeckt werden:

	T.EvadTDS	T.ManipTD	T.ManipTDTBS	T.ManipTDS	T.ManipTDSS	T.ManipTime	T.ManipTN	T.FaUpD	OSP.SecCCRS	OSP.CertSecDev	OSP.SecMod	OSP.ProtDev	OSP.ValidTDSS	OSP.Update	A.CSP	A.ProtComm	A.VerifTDS
O.Audit						x							x				
O.ExpTDS									x		x		x				
O.GenTDS				x	x						x		x				
O.IAA						x							x				
O.SecMan					x	x	x						x				
O.SecUpCP								x						x			
O.TEE	x	x	x														
O.TST				x		x											
OE.AvailAudit						x							x				
OE.CCRS	x	x							x								
OE.CSP										x					x		
OE.SecOEnv	x	x	x	x					x			x	x			x	
OE.StorMed										x							
OE.SUCP								x						x			
OE.VerifTDSS																	x